AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method of comparing access control lists to configure a security policy on a network, the method comprising the computer-implemented steps of:

identifying first sub-entries in a first access control list;

identifying second sub-entries in a second access control list;

programmatically determining whether a first access control list is functionally equivalent to a second access control list in order to configure the security policy on the network by determining whether each first sub-entry in the first access control list is equivalent to at least one of the second sub-entries; and

determining that the first access control list is functionally equivalent to the second access control list only when each of the first sub-entries is equivalent to at least one of the second sub-entries;

wherein programmatically determining whether the first access control list is equivalent to the second access control list comprises:

identifying a dimensional range for each policy action specified in the first access control list, the dimensional range of each policy action characterizing communication packets specified by entries in the first access control list for that policy action;

identifying a dimensional range for each policy action specified in the second access control list, the dimensional range of each policy action characterizing communication packets specified by entries in the second access control list for that policy action; and

determining whether the dimensional range identified for each policy action in the first access control list is equivalent to the dimensional range identified for each policy action in the second access control list;

wherein identifying the dimensional range for each policy action specified in the first access control list and in the second access control list comprises at least one step from a set of steps comprising:

identifying a source Internet Protocol (IP) address range and a destination IP address range for communication packets specified by each of the entries in the first access control list and in the second access control list;

identifying a source port range and a destination port range for communication packets specified by each of the entries in the first access control list and in the second access control list; and

identifying a communication protocol for communication packets specified by each of the entries in the first access control list and in the second access control list.

2-5. (Canceled)

6. (Previously Presented) A method as recited in Claim 1, wherein the first access control list and the second access control list each specify a plurality of entries, and each entry identifies a dimensional range for a policy action, the dimensional range characterizing communication packets that are to be affected by the policy action, and wherein programmatically determining whether a first access control list is equivalent to the second access control list includes:

determining whether each entry in the first access control list has a dimensional range that is either equivalent to or contained by the dimensional range of entries in the second access control list that specify the policy action of the entry in the first access control list.

7. (Previously Presented) A method as recited in Claim 1, wherein the first access control list and the second access control list each specify a plurality of entries, and each entry identifies a dimensional range for a policy action, the dimensional range characterizing communication packets that are to be affected by the policy action, and wherein programmatically determining whether a first access control list is equivalent to the second access control list includes:

determining whether each entry in the first access control list has a dimensional range that is either equivalent to or contained by the dimensional range of entries in

the second access control list that specify the policy action of the entry in the first access control list; and

determining whether each entry in the second access control list has a dimensional range that is either equivalent to or contained by the dimensional range of entries in the first access control list that specify the same policy action.

8. (Canceled)

9. (Currently Amended) An apparatus for ~~method of~~ comparing access control lists to configure a security policy on a network, the apparatus ~~method~~ comprising:

a processor;

a network interface that communicatively couples the processor to the network to receive flows of packets therefrom;

a memory; and

sequences of instructions in the memory which, when executed by the processor, cause the processor to carry out steps of:

identifying a dimensional range and a policy action for each entry in a first access control list;

identifying all overlapping dimensional ranges in the first access control list, each overlapping dimensional range corresponding to where the dimensional ranges of entries in the first access control list overlap;

identifying all non-overlapping dimensional ranges in the first access control list, each of the non-overlapping dimensional ranges corresponding to dimensional ranges of entries in the first access control list that do not overlap dimensional ranges of other entries in the first access control list;

identifying a policy action for each identified overlapping dimensional range of the first access control list;

identifying a policy action for each identified non-overlapping dimensional range of the first access control list; and

determining whether each identified overlapping and non-overlapping dimensional range identified from the first access control list is

contained by or equal to a dimensional range of entries in a second access control list in which the entries of the second access control list have the policy action of that identified overlapping or non-overlapping dimensional range;

wherein identifying a policy action for each identified overlapping dimensional range of the first access control list includes using a conflict rule to determine the policy action from a first policy action of a first entry having a dimensional range within the overlapping dimensional range, and from a second policy action of a second entry having a dimensional range within the overlapping dimensional range, wherein the second policy conflicts with the first policy;

wherein using the conflict rule to determine the policy action comprises selecting one of the first policy and the second policy based on a selected policy of the first and second policies being newer than an unselected policy of the first and second policies.

10. (Currently Amended) An apparatus ~~method~~ as recited in Claim 9, wherein the steps further ~~comprising~~ comprise:

identifying a dimensional range and a policy action for each entry in the second access control list;

identifying all overlapping dimensional ranges in the second access control list, each overlapping dimensional range corresponding to where the dimensional ranges of entries in the second access control list overlap;

identifying all non-overlapping dimensional ranges in the second access control list, each of the non-overlapping dimensional ranges corresponding to dimensional ranges of entries in the second access control list that do not overlap dimensional ranges of other entries in the second access control list;

identifying a policy action for each identified overlapping dimensional range in the second access control list;

identifying a policy action for each identified non-overlapping dimensional range of the second access control list; and

determining whether each identified overlapping and non-overlapping dimensional range identified from the second access control list is contained by or equal to

a dimensional range of entries in the first access control list in which the entries of the first access control list have the policy action of that identified overlapping or non-overlapping dimensional range.

11. (Currently Amended) An apparatus ~~method~~ as recited in Claim 9, wherein the steps further comprise:

identifying a dimensional range and a policy action for each entry in the second access control list;

identifying all overlapping dimensional ranges in the second access control list, each overlapping dimensional range corresponding to where the dimensional ranges of entries in the second access control list overlap;

identifying all non-overlapping dimensional ranges in the second access control list, each of the non-overlapping dimensional ranges corresponding to dimensional ranges of entries in the second access control list that do not overlap dimensional ranges of other entries in the second access control list;

identifying a policy action for each identified overlapping dimensional range of the second access control list;

identifying a policy action for each identified non-overlapping dimensional range of the second access control list; and

wherein determining whether each identified overlapping and non-overlapping dimensional range of the first access control list is contained by or equal to a dimensional range of entries in a second access control list includes determining whether each identified overlapping and non-overlapping dimensional range identified from the first access control list is contained by or equal to overlapping and non-overlapping dimensional ranges of the second access control list.

12-13. (Canceled)

14. (Currently Amended) An apparatus ~~method~~ as recited in Claim 9, wherein identifying a dimensional range and a policy action for each entry in the first access control list includes identifying a source address range and a destination address

range for communication packets specified by each of the entries in the first access control list.

15. (Currently Amended) An apparatus ~~method~~ as recited in Claim 9, wherein identifying a dimensional range and a policy action for each entry in the first access control list includes identifying a source port range and a destination port range for communication packets specified by each of the entries in the first access control list.

16. (Currently Amended) An apparatus ~~method~~ as recited in Claim 9, wherein identifying a dimensional range and a policy action for each entry in the first access control list includes identifying a communication protocol for communication packets specified by each of the entries in the first access control list.

17. (Currently Amended) A computer readable medium for comparing access control lists to configure a security policy on a network, the computer readable medium carrying instructions for performing the steps of:

identifying first sub-entries in a first access control list;

identifying second sub-entries in a second access control list;

programmatically determining whether a first access control list is functionally equivalent to a second access control list in order to configure the security policy on the network by determining whether each first sub-entry is equivalent to at least one of the second sub-entries; and

determining that the first access control list is functionally equivalent to the second access control list only when each of the first sub-entries is equivalent to at least one of the second sub-entries;

wherein programmatically determining whether the first access control list is equivalent to the second access control list comprises:

identifying a dimensional range for each policy action specified in the first access control list, the dimensional range of each policy action characterizing communication packets specified by entries in the first access control list for that policy action;

identifying a dimensional range for each policy action specified in the second access control list, the dimensional range of each policy action

characterizing communication packets specified by entries in the second access control list for that policy action; and

determining whether the dimensional range identified for each policy action in the first access control list is equivalent to the dimensional range identified for each policy action in the second access control list;

wherein identifying the dimensional range for each policy action specified in the first access control list and in the second access control list comprises at least one step from a set of steps comprising:

identifying a source Internet Protocol (IP) address range and a destination IP address range for communication packets specified by each of the entries in the first access control list and in the second access control list;

identifying a source port range and a destination port range for communication packets specified by each of the entries in the first access control list and in the second access control list; and

identifying a communication protocol for communication packets specified by each of the entries in the first access control list and in the second access control list.

18-24. (Canceled)

25. (Currently Amended) A computer system for comparing access control lists to configure a security policy on a network, the computer system comprising:

means for identifying first sub-entries in a first access control list;

means for identifying second sub-entries in a second access control list;

means for programmatically determining whether a first access control list is functionally equivalent to a second access control list in order to configure the security policy on the network by determining whether each first sub-entry is equivalent to at least one of the second sub-entries; and

means for determining that the first access control list is functionally equivalent to the second access control list only when each of the first sub-entries is equivalent to at least one of the second sub-entries;

wherein the means for programmatically determining whether the first access control list is equivalent to the second access control list comprise:

means for identifying a dimensional range for each policy action specified in the first access control list, the dimensional range of each policy action characterizing communication packets specified by entries in the first access control list for that policy action;

means for identifying a dimensional range for each policy action specified in the second access control list, the dimensional range of each policy action characterizing communication packets specified by entries in the second access control list for that policy action; and

means for determining whether the dimensional range identified for each policy action in the first access control list is equivalent to the dimensional range identified for each policy action in the second access control list;

wherein the means for identifying the dimensional range for each policy action specified in the first access control list and the means for identifying the dimensional range for each policy action specified in the second access control list comprises at least one means from a set of means comprising:

means for identifying a source Internet Protocol (IP) address range and a destination IP address range for communication packets specified by each of the entries in the first access control list and in the second access control list;

means for identifying a source port range and a destination port range for communication packets specified by each of the entries in the first access control list and in the second access control list; and

means for identifying a communication protocol for communication packets specified by each of the entries in the first access control list and in the second access control list.

26. (Currently Amended) A policy server communicatively coupled to security devices in a network to configure a security policy on a network, the policy server comprising:

a processor;

a network interface that communicatively couples the processor to the network to receive flows of packets therefrom;

a memory; and

sequences of instructions in the memory which, when executed by the processor, cause the processor to carry out the steps of:

identifying first sub-entries in a first access control list;

identifying second sub-entries in a second access control list;

programmatically determining whether a first access control list is functionally equivalent to a second access control list in order to configure the security policy on the network by determining whether each first sub-entry is equivalent to at least one of the second sub-entries; and

determining that the first access control is functionally equivalent to the second access control list only when each of the first sub-entries is equivalent to at least one of the second sub-entries;

wherein programmatically determining whether the first access control list is equivalent to the second access control list comprises:

identifying a dimensional range for each policy action specified in the first access control list, the dimensional range of each policy action characterizing communication packets specified by entries in the first access control list for that policy action;

identifying a dimensional range for each policy action specified in the second access control list, the dimensional range of each policy action characterizing communication packets specified by entries in the second access control list for that policy action; and

determining whether the dimensional range identified for each policy action in the first access control list is equivalent to the dimensional range identified for each policy action in the second access control list;

wherein identifying the dimensional range for each policy action specified in the first access control list and in the second access control list comprises at least one step from a set of steps comprising:

identifying a source Internet Protocol (IP) address range and a destination IP address range for communication packets specified by each of the entries in the first access control list and in the second access control list;

identifying a source port range and a destination port range for communication packets specified by each of the entries in the first access control list and in the second access control list; and

identifying a communication protocol for communication packets specified by each of the entries in the first access control list and in the second access control list.

27. (Currently Amended) The policy server of claim 26, ~~wherein~~ further comprising a memory to store a plurality of access control lists, including the first access control list and the second access control list, and wherein the processor is configured to configure each security device on the network with at least one of the plurality of access control lists.

28. (Canceled)

29. (New) A computer system as recited in Claim 25, wherein the first access control list and the second access control list each specify a plurality of entries, and each entry identifies a dimensional range for a policy action, the dimensional range characterizing communication packets that are to be affected by the policy action, and wherein the means for programmatically determining whether a first access control list is equivalent to the second access control list comprise:

means for determining whether each entry in the first access control list has a dimensional range that is either equivalent to or contained by the dimensional range of entries in the second access control list that specify the policy action of the entry in the first access control list.

30. (New) A computer system as recited in Claim 25, wherein the first access control list and the second access control list each specify a plurality of entries, and each entry identifies a dimensional range for a policy action, the dimensional range characterizing communication packets that are to be affected by the policy action, and wherein the means for programmatically determining whether a first access control list is equivalent to the second access control list comprise:

means for determining whether each entry in the first access control list has a dimensional range that is either equivalent to or contained by the dimensional range of entries in the second access control list that specify the policy action of the entry in the first access control list; and

means for determining whether each entry in the second access control list has a dimensional range that is either equivalent to or contained by the dimensional range of entries in the first access control list that specify the same policy action.

31. (New) A policy server as recited in Claim 26, wherein the first access control list and the second access control list each specify a plurality of entries, and each entry identifies a dimensional range for a policy action, the dimensional range characterizing communication packets that are to be affected by the policy action, and wherein programmatically determining whether a first access control list is equivalent to the second access control list comprises:

determining whether each entry in the first access control list has a dimensional range that is either equivalent to or contained by the dimensional range of entries in the second access control list that specify the policy action of the entry in the first access control list.

32. (New) A policy server as recited in Claim 26, wherein the first access control list and the second access control list each specify a plurality of entries, and each entry identifies a dimensional range for a policy action, the dimensional range characterizing communication packets that are to be affected by the policy action, and wherein programmatically determining whether a first access control list is equivalent to the second access control list comprises:

determining whether each entry in the first access control list has a dimensional range that is either equivalent to or contained by the dimensional range of entries in the second access control list that specify the policy action of the entry in the first access control list; and

determining whether each entry in the second access control list has a dimensional range that is either equivalent to or contained by the dimensional range of entries in the first access control list that specify the same policy action.